# ALICE’SBIRTHDAYPARTY– PART1

本题为RSA共模攻击实现，已知密文c1,c2,其对应明文相同，使用不同e(e1,e2)加密，但使用的N相同，已知e1,e2,N求明文m

数据见文件mtc3-kitrub-01-alicebirthday-add.txt

程序运行所需数据已包含进代码，其中c1,c2为密文base64编码后转化为十六进制对应的十进制大数。

实现原理为：

令c1\*s1+c2\*s2=1,则有

c1s1\*c2s2 = m

输出为base64解码后的明文。

网站对答案的认证截图如cache.jpg所示。